

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Kempin, Christopher Serial No. 10/712,677 Filed: 11/13/2003 For: “Network Endpoint Health Check”	Group Art Unit: 2153 Examiner: PHAN, Tuankhanh D. Customer Number: 25854
--	---

APPEAL BRIEF

Commissioner for Patents
Mail Stop Amendment
P.O. Box 1450
Alexandria, VA 22313-1450

May 2, 2008

Sir,

Pursuant to 37 C.F.R. § 41.37, Applicant submits its Appeal Brief according to the following Table of Contents:

Real Party in Interest	2
Related Appeals and Interferences	2
Status of Claims	2
Status of Amendments	2
Summary of Claimed Subject Matter	2
Grounds of Rejection to be Reviewed on Appeal	5
Argument	5
Summary of Arguments.....	5
Detailed Arguments and Citations to Authority	6
Conclusion	9
Claims Appendix	10
Evidence Appendix.....	14
Related Proceedings Appendix	15

REAL PARTY IN INTEREST

The real party in interest in the present application and Appeal is: International Business Machines Corporation, Armonk, New York 10504.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims **1-11** are pending.

Claims **1-11** stand rejected.

Claims **1-11** are subject to the present appeal.

STATUS OF AMENDMENTS

Applicant filed amendments to Claims 10 and 11 in response to the Final Rejection of the last Office Action. The amendments were entered for purposes of appeal per the Advisory Action mailed on December 31, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

Specifically, the independent claims are summarized as follows:

Claim 1:

Claim 1 is directed to a system for monitoring the integrity of a plurality of endpoints and

a communication channel (FIG. 1, item 118) between the plurality of endpoints (*Id.*, *e.g.*, item 102) and a gateway device (*Id.*, *e.g.*, item 112, *see, also*, ¶[0008]) in which a monitoring application monitors the integrity of the endpoint (¶[0017]). At a predetermined time the the monitoring application sends a periodic signal through a communication channel to the gateway device indicating the integrity of the endpoint (¶[0017]). A server has a centralized database listing a status of the endpoint (¶[0020]). A gateway device is in communication with the server and the endpoint (¶[0017]). The gateway device include a monitored list (FIGS. 2, 3) that lists the status of the endpoint in communication with the gateway device (¶[0018]). The gateway device is configured to send a state change message to the server when the gateway device fails to receive a periodic signal from the endpoint and if the status of the endpoint is either in a Healthy state, which indicates the endpoint is functioning properly, or a Trouble state, which indicates the endpoint has failed once (¶[0022]). The gateway device is also configured not to send the state change message to the server upon a failure to receive the periodic signal from the endpoint when the status of the endpoint is in a Removed state, which indicates the endpoint has been removed from the monitored list (¶[0023]).

Claim 7:

Claim 7 is directed to a method for monitoring the integrity of an endpoint and a data channel between the endpoint and a gateway device (¶[0008]). The system determines a health of an endpoint and if the endpoint is in a Healthy state, which indicates the endpoint is functioning properly, a periodic signal is sent at a predetermined time through the data channel to the gateway device associated with the endpoint (¶[0017]). If the gateway device fails to receive a periodic signal from the endpoint and if the status of the endpoint in a monitored list in the gateway device is the Healthy state, the status of the endpoint in the monitored list is set to a Trouble state, which indicates the endpoint has failed once, and a state change signal is sent to a server indicating the status of the endpoint has been set to the Trouble state (¶[0022]). If the gateway device fails to receive a periodic signal from the endpoint and if the status of the endpoint in a monitored list in the gateway device is the Trouble state, the status of the endpoint

in the monitored list is set to a Removed state, which indicates the endpoint has been removed from the monitored list, and a state change signal is sent to the server indicating the status of the endpoint has been set to the Removed state (§[0023]).

Claim 10:

Claim 10 is directed to a method for monitoring the integrity of an endpoint and a data channel between the endpoint and a gateway device (§[0008]). A status of an endpoint in a monitored list in the gate device is determined (§[0017]). If the status of the endpoint is either a Healthy state, which indicates the endpoint is functioning properly, or a Trouble state, which indicates the endpoint has failed once, a timer for an endpoint listed in a monitored list in the gateway device is set (§[0018]). If the timer expires and the status of the endpoint in the monitored list is in the Healthy state, setting the status of the endpoint to the Trouble state and sending a first state change message to a server (§[0022]). If the timer expires and the status of the endpoint in the monitored list is in the Trouble state, the status of the endpoint is set to a Removed state, which indicates the endpoint has been removed from the monitored list, and a second state change message is sent to the server (§[0023]). If a periodic message is received from the endpoint the timer is reset (§[0024]).

Claim 11:

Claim 11 is directed to a system for monitoring the integrity of a plurality of endpoints and a communication channel between the plurality of endpoints and a gateway device (§[0008]). An endpoint means has a monitoring means for monitoring the integrity of the endpoint means. The monitoring means at a predetermined time sends a periodic signal through a communication means to the gateway device indicating the integrity of the endpoint means (§[0017]). A server means has a centralized database means listing the status of the endpoint means (§[0020]). A gateway means is in communication with the server means and with the endpoint means (§[0017]). The gateway means includes a monitored list listing the status of the endpoint means in communication with the gateway means (§[0018]). The gateway means is

configured to send a state change message to the server means when the gateway means fails to receive a periodic signal from the endpoint means and if the status of the endpoint means is either a Healthy state, which indicates the endpoint is functioning properly, or a Trouble state, which indicates the endpoint has failed once ([0022]). The gateway means is further configured not to send the state change message to the server means upon a failure to receive the periodic signal from the endpoint means when the status of the endpoint means in the monitored list is a Removed state, which indicates the endpoint has been removed from the monitored list ([0023]).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are to be reviewed on appeal:

1. Claims 1-6 and 11 stand rejected under 35 U.S.C. § 112, second paragraph.
2. Claims 1-11 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application No. 2004/0010716 (“Childress et al.”).

ARGUMENT

A. SUMMARY OF ARGUMENTS.

This section summarizes Applicant’s arguments. A more detailed argument and citation to authority is found below.

Claim Rejection under 35 U.S.C. §112, second paragraph

1. The final Office Action improperly rejects the claims for using negative limitations.

The final Office Action rejects Claims 1 and 11 under 35 U.S.C. §112, second paragraph

on the grounds that the claims include limitations reciting that “the gateway device is ‘capable of not’ sending state change.” However, this type of limitation is specifically “perfectly acceptable” pursuant to MPEP § 2173.05(g).

2. The final Office Action improperly rejects the claims for using functional limitations.

The final Office Action rejects Claims 1-6 and 11 under 35 U.S.C. §112, second paragraph on the grounds that the claims “are narrative in form and replete with indefinite and functional or operational language.” However, the final Office Action fails to demonstrate how the cited language is indefinite. Furthermore, “[f]unctional language does not, in and of itself, render a claim improper,” pursuant to MPEP § 2173.05(g).

Claim Rejection under 35 U.S.C. §102

1. The final Office Action fails to demonstrate that each element of the claims rejected under § 102 are disclosed in the cited reference.

The final Office Action rejects Claims 1-11 under 35 U.S.C. §102(b) as being anticipated by Childress. However, the final Office Action fails to demonstrate that the all of the limitations of the rejected claims are found in the Childress reference.

B. DETAILED ARGUMENTS AND CITATIONS TO AUTHORITY.

Regarding the Claim Rejection under 35 U.S.C. §112, second paragraph:

Claims 1-6 and 11 were rejected under 35 U.S.C. § 112, for failing to define the invention. As grounds for the rejection, the final Office Action stated that: (1) it is unclear how the limitation of the gateway device not being capable of sending a state change message limited the claim; and (2) “[t]he claims are narrative in form and replete with indefinite and functional or

operational language.” As will be demonstrated below, neither of these grounds are sufficient to sustain this rejection.

Regarding the first assertion, when the cited portion of the claims is taken in its full context, it is clear how the claims are limited. The Specification clearly indicates that an endpoint can be in one of only three states: Healthy, Trouble or Removed. (*See, e.g.*, FIGS. 2, 3 and Specification, ¶[0018]) The independent claims recite that, upon failure to receive a periodic signal from an endpoint device, the gateway device is configured *to* send a state change message when the endpoint is in either the Healthy or the Trouble state. Otherwise, when the endpoint is in the Removed state, the gateway device is configured *not to* send the state change message. Each possible state is addressed and an action (or inaction) is associated with each state. When taken in its full context, the meets and bounds of this limitation are perfectly clear.

Furthermore, the MPEP makes it clear that this type of limitation is perfectly acceptable. *In re Barr*, 444 F.2d 588 (CCPA 1971) held that “the limitation used to define a radical on a chemical compound as ‘incapable of forming a dye with [an] oxidizing agent’ although functional, was perfectly acceptable because it set definite boundaries on the patent protection sought.” MPEP § 2173.05(g). Analogously, the amended claims make it clear that the gateway is incapable of sending a state change message when the endpoint is in the Removed state and, thus, sets definite boundaries on the patent protection sought. Therefore, the cited limitations are definite for the same reasons that the cited limitation in *In re Barr* was held to be definite. For this reason, the §112 rejection should not be sustained.

Regarding the second assertion in the final Office Action, the MPEP clearly states that “functional language ... does not render a claim improper.” MPEP § 2173.05(g) While the final Office Action rejects the claims on the grounds that they include functional language, it provides no reasoning to support the rejection. The MPEP clearly allows for functional language of the type recited in the rejected claims. For this reason, also, the §112 rejection should not be sustained.

Regarding the Claim Rejection under 35 U.S.C. §102:

1. The final Office Action fails to demonstrate that each element of the claims rejected under § 102 are disclosed in the cited reference.

“[F]or anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present.” MPEP 706.02. A rejection under 35 U.S.C. §102(b) requires that each element of the rejected claim be found in the cited reference.

The final Office Action rejects Claims 1-11 under 35 U.S.C. §102(e), as being anticipated by Childress. However, the rejected claims include elements not disclosed in Childress. Applicant, in its Response to the final Office Action, pointed out that the cited passage of Childress (§[0096]) fails to disclose the limitation that requires the gateway device *not* to send the state change message to the server when the status of the endpoint is in the Removed state and explained why. Paragraph [0096] of Childress merely states:

Event_Severity—This string corresponds to the TEC severity levels (HARMLESS, WARNING, CRITICAL and FATAL) and must always be in uppercase. This TEC severity level is the TEC severity level to which the incident severity level maps to;

While the cited paragraph uses the word “FATAL,” there is no indication in this paragraph (or anywhere else in Childress) that an endpoint being in a Removed state results in a state change message being suppressed by the gateway device. Any assertion that use of the term “FATAL” means suppression of a state change message is mere speculation, and is certainly not sufficient to support a §102 rejection.

In response to this argument, the Advisory Action states:

Applicant argues healthcheck modules that are applied to managed nodes (not endpoints) in a program will not run if a managed node is down. Applicant tries to differentiate between ‘managed nodes’ and ‘endpoints.’

Response: There is no distinction between a “manage node” and an “endpoint.” A manage node could be an end user or a thin client station, therefore it is an endpoint...


This statement completely fails to address the question of whether Childress discloses the limitations of the gateway device being configured *to* send a state change message when the endpoint is in either the Healthy or the Trouble state and being configured *not to* send a state change message when the endpoint is in the Removed state. Childress simply does not disclose these limitations and the final Office Action, along with the Advisory Action completely fail to demonstrate otherwise. For this reason, the §102(e) rejection should not be sustained.

CONCLUSION

For the reasons enumerated above, Applicant believes that the rejections were in error and requests that all rejections be reversed and that all remaining claims be allowed.

No addition fees are believed due. However, the Commissioner is hereby authorized to charge any additional fees which may be required, including any necessary extensions of time, which are hereby requested, to Deposit Account No. 503535.

May 2, 2008
Date



Bryan W. Bockhop
Registration No. 39,613

Customer Number: 25854

Bockhop & Associates, LLC
2375 Mossy Branch Dr.
Snellville, GA 30078

Tel. 678-919-1075
Fax 678- 749-7314
E-Mail: bwb@bockpatent.com

Claims Appendix

LISTING OF CLAIMS

1. A system for monitoring the integrity of a plurality of endpoints and a communication channel between the plurality of endpoints and a gateway device, comprising:
 - an endpoint having a monitoring application for monitoring the integrity of the endpoint, the monitoring application at a predetermined time sending a periodic signal through a communication channel to the gateway device indicating the integrity of the endpoint;
 - a server having a centralized database listing a status of the endpoint; and
 - a gateway device in communication with the server and with the endpoint, the gateway device including a monitored list listing the status of the endpoint in communication with the gateway device, the gateway device being configured to send a state change message to the server when the gateway device fails to receive a periodic signal from the endpoint and if the status of the endpoint is either in a Healthy state, which indicates the endpoint is functioning properly, or a Trouble state, which indicates the endpoint has failed once, the gateway device further being configured not to send the state change message to the server upon a failure to receive the periodic signal from the endpoint when the status of the endpoint is in a Removed state, which indicates the endpoint has been removed from the monitored list.
2. The system of claim 1, wherein the periodic signal is sent through a data channel connecting the endpoint and the gateway.
3. The system of claim 1, wherein the status of the endpoint is set to the Trouble state when the gateway device fails to receive the periodic signal from the endpoint and the status of the endpoint is in the Healthy state.

4. The system of claim 1, wherein the status of the endpoint is set to the Removed state when the gateway device fails to receive the periodic signal from the endpoint and the status of the endpoint is in the Trouble state.

5. The system of claim 1, wherein the centralized database has a plurality of entries, each entry being associated with one endpoint, the status of the endpoint, and the gateway device associated with the endpoint.

6. The system of claim 1 further comprising a timer, wherein the timer is associated with the endpoint.

7. A method for monitoring the integrity of an endpoint and a data channel between the endpoint and a gateway device, comprising the steps of:

determining a health of an endpoint;

if the endpoint is in a Healthy state, which indicates the endpoint is functioning properly, sending a periodic signal at a predetermined time through the data channel to the gateway device associated with the endpoint;

if the gateway device fails to receive a periodic signal from the endpoint and if the status of the endpoint in a monitored list in the gateway device is the Healthy state, setting the status of the endpoint in the monitored list to a Trouble state, which indicates the endpoint has failed once, and sending a state change signal to a server indicating the status of the endpoint has been set to the Trouble state; and

if the gateway device fails to receive a periodic signal from the endpoint and if the status of the endpoint in a monitored list in the gateway device is the Trouble state, setting the status of the endpoint in the monitored list to a Removed state, which indicates the endpoint has been removed from the monitored list, and sending a state change signal to the server indicating the status of the endpoint has been set to the Removed state.

8. The method of claim 7, further comprising the steps of:
 - determining if a timer associated with the endpoint has expired;
 - if the timer has expired, determining the status of the endpoint associated with the timer;
 - if the status of the endpoint is the Healthy state, setting the status of the endpoint to the Trouble state;
 - if the status of the endpoint is the Trouble state, setting the status of the endpoint to the Removed state; and
 - resetting the timer.
9. The method of claim 7, further comprising the steps of:
 - receiving a configuration signal from the endpoint;
 - determining if the endpoint is listed in the monitored list; and
 - if the endpoint is not listed in the monitored list, adding the endpoint to the monitored list and transmitting a configuration signal to the server.
10. A method for monitoring the integrity of a an endpoint and a data channel between the endpoint and a gateway device, comprising the steps of:
 - determining a status of an endpoint in a monitored list in the gate device;
 - if the status of the endpoint is either a Healthy state, which indicates the endpoint is functioning properly, or a Trouble state, which indicates the endpoint has failed once, setting a timer for an endpoint listed in a monitored list in the gateway device;
 - if the timer expires and the status of the endpoint in the monitored list is in the Healthy state, setting the status of the endpoint to the Trouble state and sending a first state change message to a server;
 - if the timer expires and the status of the endpoint in the monitored list is in the Trouble state, setting the status of the endpoint to a Removed state, which indicates the endpoint has been removed from the monitored list, and sending a second state change message to the server; and
 - resetting the timer if a periodic message is received from the endpoint.

11. A system for monitoring the integrity of a plurality of endpoints and a communication channel between the plurality of endpoints and a gateway device, comprising:

an endpoint means having a monitoring means for monitoring the integrity of the endpoint means, the monitoring means at a predetermined time sending a periodic signal through a communication means to the gateway device indicating the integrity of the endpoint means;

a server means having a centralized database means listing the status of the endpoint means; and

a gateway means in communication with the server means and with the endpoint means, the gateway means including a monitored list listing the status of the endpoint means in communication with the gateway means, the gateway means being configured to send a state change message to the server means when the gateway means fails to receive a periodic signal from the endpoint means and if the status of the endpoint means is either a Healthy state, which indicates the endpoint is functioning properly, or a Trouble state, which indicates the endpoint has failed once, the gateway means further configured not to send the state change message to the server means upon a failure to receive the periodic signal from the endpoint means when the status of the endpoint means in the monitored list is a Removed state, which indicates the endpoint has been removed from the monitored list.

Evidence Appendix

(None)

Related Proceedings Appendix

(None)